Le droit d'internet

Poullet, Yves; Montero, Etienne

Published in:
Signes du temps

Publication date:
1997

Document Version
le PDF de l'éditeur

Le droit d'Internet : un mirage ?

Yves POULLET et Etienne MONTERO,

Faculté de droit, Facultés Universitaires Notre-Dame de la Paix à Namur

Ainsi, nous voilà en marche vers la société de l'information dont Internet constitue la préfiguration. Quelques mots clés caractérisent ce "réseau des réseaux": la digitalisation (technique consistant à représenter, transmettre et stocker toutes les informations quel qu'en soit le type -image, sons, données- sous forme de signaux binaires, les bits); la *grande capacité du réseau*, grâce aux technologies de compression, ce qui explique que demain convergeront les télécommunications et l'audiovisuel; *l'évolution vers des applications économiques et commerciales:* Internet n'est plus seulement la "foire aux idées" des scientifiques universitaires, il est surtout la foire commerciale, qui permet l'achat de biens et de services; *l'extension mondiale d'Internet*, le "village global" où l'internaute peut franchir en quelques secondes les frontières, l'espace virtuel se jouant des frontières; le *caractère ouvert* du réseau complète cette dimension globale d'Internet. L'internaute, hypertexte aidant, navigue sur cette toile d'araignée d'un site à l'autre par des chemins chaque fois différents.

Dans ce contexte, comment envisager le rôle du Droit? Certes, les réglementations ne manquent pas. Le commerce en ligne vis-à-vis des particuliers n'est jamais qu'une forme de vente à distance et on connaît les multiples règles de protection des consommateurs qui régissent ce genre d'opération. La législation pénale punit la réception et l'émission de messages pédophiles y compris via Internet.

La réglementation ne fait pas défaut mais sans doute son identification et surtout son application s'avèrent malaisées. Quel droit appliquer à un site dont la localisation est incertaine et volatile? L'affaire du livre du docteur Gübler, mis sur Internet en violation des droits d'auteur et du respect de la vie privée du Président Mitterrand, n'illustre-t-elle pas l'impuissance du juge qui, au moment où il ordonnait la saisie du serveur indélicat, savait pertinemment que l'ouvrage avait déjà fait le tour du monde.

Notre propos ne peut aborder l'ensemble des questions juridiques soulevées par Internet[1]. Qu'il nous suffise d'attirer l'attention sur deux points: la protection de la vie privée, d'une part, les responsabilités des acteurs d'Internet à raison, notamment, du contenu des messages diffusés.

Internet et le respect de la vie privée

Les risques - les enjeux

La notion de vie privée ne se réduit pas à la protection de quelques données relatives à la vie dite intime: elle vise, plus largement, la maîtrise par l'individu des informations qui circulent à son propos, la maîtrise de son "image informationnelle ".

Internet remet en cause cette maîtrise de diverses manières. En premier lieu, le faible coût de la mise sur pied des sites explique la multiplication des bases de données contenant des informations nominatives dont l'accessibilité est facilitée et peut s'opérer de tous les points du globe. On ajoute que les moteurs de recherche puissants de type Yahoo, Altavista... permettent de repérer les multiples manifestations d'expression ou la présence sur les sites de tel ou tel personnage et de mieux cerner le profil type.

Ensuite, la tentation est grande pour les internautes de multiplier les informations personnelles à leur propos pour donner à leurs pages Web un aspect plus convivial voire amical, ceci sans s'inquiéter des utilisations possibles et incontrôlables qui seront faites de cette image.

Au-delà, il va de soi que, suite à l'accès à un site particulier, l'internaute, qui a pu révéler son nom et son adresse, livre de l'information non seulement par le contenu des messages qu'il adresse, mais également par la façon dont il consulte les pages du site, le temps consacré à la lecture de telle ou telle page, le site de provenance et celui vers lequel il s'oriente. Autant d'informations qui permettent au serveur de mieux connaître les goûts et les habitudes de consultation de l'internaute qui s'adresse à lui.

Plus graves, enfin, les traitements dits invisibles, c'est-à-dire opérés en dehors de la conscience de l'individu. Les plus connus sont opérés par le truchement de "cookies", c'est-à-dire des informations que le serveur stocke sur le disque de l'utilisateur sans que celui-ci soit prévenu. Le serveur peut également interroger le fichier de cookies qui se trouve sur le disque dur de l'utilisateur. Mais le serveur peut également récupérer l'historique des pages Web que vous avez consultées. Cette fonctionnalité est utilisée par les sociétés de marketing direct pratiquant le "one-to-one marketing" afin de cibler les utilisateurs et d'enregistrer dans des bases des profils précis d'habitudes, réflexes, goûts et centres d'intérêts dans le but de générer dans les pages Web que consulte l'utilisateur des publicités très ciblées. Cela pose un important problème de respect de la vie privé.

L'utilisation des multiples fonctionnalités du réseau Internet, accentue les risques d'atteinte à la protection des données, de par les caractéristiques du réseau:

- l'ouverture du réseau et les grandes facilités de réutilisation des données y circulant suscitent les craintes d'utilisations des données incompatibles avec la finalité qui a présidé à l'envoi du message. En outre, l'ouverture du réseau rend incontrôlables la circulation des informations et leurs utilisateurs;

- l'internationalisation des flux, favorisée par la large diffusion du standard Internet et par le faible coût d'utilisation de ce réseau, entraîne la peur de voir la protection proposée par certaines réglementations s'évanouir au fil des chemins lointains parcourus par les messages;

- enfin, l'interactivité du réseau et surtout son mode de fonctionnement fondé sur l'activation des hyperliens justifient l'attention portée aux risques liés au traçage des utilisations du www et aux possibilités infinies d'espionnage que l'envoi de programmes sur le système d'informations de l'utilisateur permet.

Les solutions

Elles sont de deux ordres: le droit, en particulier la directive 95/46 CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données fixe quelques principes dont le respect permettrait d'assurer la protection des données (a). Cependant, il faut bien reconnaître que le droit en la matière n'atteindra son but que s'il trouve dans la technique une alliée (b).

(a) la solution réglementaire

Sans pouvoir procéder à une analyse complète de la directive, relevons l'intérêt de l'application de quelques principes.

Internet représente à la fois un outil de collecte d'informations et de communication entre la personne concernée et le responsable du traitement. Cette double fonction, présente dans un même média, permet de rendre plus effectives certaines dispositions de la directive. On songe en particulier à la manière dont le principe de transparence, les droits d'accès, de correction pourraient s'exercer, à moindre coût, via Internet.

«Un nouvel espace-temps» *in* «Des autoroutes de l'information au cyberespace»,

Serge Fdida, Flammarion, 1997, pp. 108-110.

«(...) L'information a un coût puisqu'elle possède une valeur marchande. L'accès à l'information renforce-t-il les différences qui existent déjà entre les pauvres et les riches, les pays du Nord et ceux du Sud? Les récentes études réalisées pour identifier le profil type de l'internaute montrent qu'il est essentiellement un homme (70 %) aux revenus significatifs (320 000 F par an). La généralisation de l'accès au réseau demande alors le financement d'une infrastructure permettant aux pays pauvres ou en voie de développement de participer à ce mouvement. Jusqu'à récemment, ces infrastructures étaient financées par des institutions ou par les gouvernements. Elles seront progressivement relayées par des opérateurs privés qui développeront leurs réseaux en fonction des revenus espérés en irriguant certaines portions de la population. Le financement de ces routes électroniques dans les pays pauvres est un problème important, mais qui n'est pas nouveau.

A l'heure où le G7 (groupement des sept pays les plus industrialisés) porte sa réflexion sur la société globale de l'information, le taux d'équipement en postes téléphoniques est dérisoire dans les pays du Sud, et il est souvent rappelé qu'il y a plus de téléphones à Manhattan que dans tous les pays de l'Afrique noire réunis. Il ne faut pas espérer que les technologies de l'information résoudront les nombreux problèmes actuels. Avant d'envisager une pénétration de l'Internet dans ces pays, il faut d'abord ramener le taux d'équipement d'autres services comme l'eau, l'électricité ou le téléphone à un niveau acceptable.

Cependant, même si l'accès banalisé aux autoroutes de l'information ne constitue pas une priorité pour ces pays, elles doivent être accessibles en des points stratégiques tels que certaines institutions, les universités, des centres industriels, afin de garantir l'accès aux informations sans lesquelles aujourd'hui l'exclusion est garantie. Pour ce qui est de l'Internet, le mouvement est en marche dans les pays d'Amérique du Sud et d'Europe de l'Est. Des initiatives émergent en Afrique mais se heurtent toujours à de fortes difficultés. Ces dernières constituent certainement un frein au développement de l'accès à l'information pour les pays du tiers-monde, mais la connexion de certaines institutions locales leur permettrait d'accéder à la bibliothèque électronique, d'aider la formation des compétences localement, d'entretenir le tissu scientifique et de limiter en partie la fuite des cerveaux. (...)»

Au-delà, la configuration des écrans pourrait permettre à l'internaute de connaître à tout moment l'identité du responsable, les finalités poursuivies par celui-ci voire, via un lien hypertexte, les dispositions réglementaires ou autoréglementaires que le responsable s'engage à suivre[2].

L'interactivité du média ouvre d'autres possibilités encore, notamment celle de déterminer les utilisations de données auxquelles l'utilisateur consent, et ce en cochant des cases apparaissant à l'écran avant la collecte des données, la possibilité d'exercer a priori son droit d'opposition, etc.

Le principe de la collecte et du traitement loyaux s'applique aux traitements réalisés via Internet. L'article 6, 1, a) de la directive, qui exige que la collecte et l'utilisation de données soient faites de manière loyale, exclut des pratiques comme celles dénoncées dans la première section à propos des traitements invisibles.

Par ailleurs, selon l'article 6, 1, b), l'utilisation des données doit être "compatible" avec la ou les finalités annoncées lors de la collecte des données, c'est-à-dire rentrer dans le champ des utilisations raisonnablement attendues par la personne concernée à la lecture des finalités annoncées par le responsable du traitement.

Quelques exemples illustrent cette notion: en participant à un forum public de discussion relatif à la cryptographie, une personne peut s'attendre à ce que des invitations lui soient envoyées à propos de conférences ou séminaires en la matière; par contre, le consommateur qui visite le site d'un supermarché sur Internet ne peut raisonnablement pas s'attendre à ce qu'une firme tierce sur base de l'analyse de son profil de personnalité lui propose l'achat d'ouvrages ou la participation à tel ou tel voyage, comme cela pourrait être le cas si les deux entreprises participent à un système commun d'analyse du comportement de l'utilisateur comme "double click".

On ajoutera que la Directive oblige, sous réserve d'exceptions, les Etats membres à interdire le transfert des données personnelles vers des pays ne disposant pas de "protection adéquate". Cette disposition permettrait de restreindre l'accès à des sites localisés sur des territoires n'offrant aucune protection des données. Mais l'énoncé même de cette assertion laisse le citoyen sceptique: comment rendre effective une telle disposition dans un cyberespace où aucune autorité ne peut contrôler tous les chemins possibles que peut emprunter l'internaute sur cette toile d'araignée de dimension mondiale.

(b) les solutions techniques

Diverses solutions techniques sont généralement avancées[3]. Elles répondent à des soucis divers.

Les premières visent à garantir la confidentialité des messages exprimés par les utilisateurs; les deuxièmes, à garantir ce dernier contre les intrusions venant de l'extérieur; les troisièmes, contre les pratiques des destinataires des messages. En ce sens, elles sont complémentaires. Les premières tournent autour de l'encryptage, qu'ils s'agisse de l'encryptage lui-même, du remailing ou de la possibilité de surfing anonyme (1); les secondes combattent les traitements invisibles dont nous avons parlé dans la première partie (2); les troisièmes utilisent des techniques de filtrage pour contrôler les pratiques des serveurs en matière de vie privée (3).

1. les techniques d'encryptage

Fortement recommandées par les commissaires à la protection des données, elles consistent tantôt simplement à celer le message, tantôt à éviter même la possibilité d'identifier son auteur en passant par un tiers (un remailer, ou réexpéditeur) qui prendra soin de dissimuler l'adresse de l'émetteur.

2. Les protections contre les traitements invisibles

Certains logiciels installés dans le navigateur permettent soit de refuser systématiquement toute information excédant la réponse à la requête de l'utilisateur et donc les cookies, soit d'alerter l'utilisateur de l'envoi de ceux-ci par un serveur contacté et de lui permettre de s'opposer à sa réception.

3. L'information préalable sur les pratiques du serveur et les préférences de l'utilisateur en matière de vie privée

Ce troisième type de solutions techniques poursuit un objectif différent des deux premiers types: il ne s'agit ni de protéger la confidentialité d'un message ni de lutter contre des traitements invisibles mais, d'une part, de permettre à l'utilisateur de sélectionner les sites visités après lui avoir donné une information sur les pratiques du serveur et d'autre part, le cas échéant, de permettre à l'utilisateur d'indiquer au serveur quelles conditions relatives à la protection de ses données il entend voir respecter.

Internet et les responsabilités

Internet est un outil de communication aux mains des hommes; à ce titre, il sert pour le meilleur et pour le pire. Il favorise les échanges entre personnes géographiquement éloignées et une diffusion des connaissances à plus grande échelle... Il offre de réelles possibilités d'épanouissement pour l'individu (à condition de veiller à la qualité des contenus proposés), mais il permet aussi à la malice humaine de s'exprimer dans des formes nouvelles et de donner à ses crimes une portée planétaire. Il n'y a pas

lieu de s'en étonner: depuis que l'humanité existe, toutes les inventions, toutes les avancées technologiques entraînent leur lot de comportements répréhensibles.

La méchanceté est parfois imaginative, mais pas toujours. Ainsi, Internet peut être l'instrument d'abus relativement spécifiques, en ce sens qu'ils ont pour cibles des biens de l'informatique. On parle, dans ce cas, de "fraude ou criminalité informatique", à moins d'utiliser un néologisme dans le vent tel que cyber-terrorisme. Les comportements répréhensibles sont diversifiés: entrée par effraction dans un système informatique, manipulation ou destruction de données, pillage de données, piratage de programmes, envoi d'un virus, etc. Mais, Internet peut être aussi le support d'infractions tout à fait conventionnelles, qui peuvent se commettre par d'autres moyens: atteintes à l'honneur et à la bonne réputation (diffamation, calomnie...); diffusion d'informations à caractère pornographique ou pédophile, raciste ou violent; contrefaçon de droits d'auteur; violation du secret de l'instruction, du droit à l'image; etc.

Une criminalité relativement originale donc et une criminalité plus classique, qui tire parti de la couverture mondiale du nouveau média. Pour faire face à la première, notre droit est, à ce jour, totalement désarmé. D'autres pays tels que la France ou les Pays-Bas ont déjà légiféré pour incriminer et sanctionner les différentes manifestations de la fraude informatique. La Belgique est à la traîne sur ce point.

En revanche, notre droit pénal est globalement apte à protéger les utilisateurs d'Internet contre ceux qui s'en servent pour commettre des infractions classiques. Plusieurs infractions tombent clairement sous l'application de dispositions du Code pénal formulées en termes suffisamment larges. Ainsi, il est clair que celles concernant les atteintes portées à l'honneur ou à la considération des personnes (art. 443 et s.) s'appliquent aux messages à caractère calomnieux, diffamatoire ou injurieux véhiculés par Internet. Les dispositions relatives à la corruption de la jeunesse (art. 379 et s.) visent pareillement toute une série d'abus (incitations à la débauche de mineurs, promotion de la pédophilie, publicité en faveur du tourisme sexuel...) sans opérer de distinction entre les supports de cette diffusion.

Dans d'autres hypothèses, les juges ont parfois été amenés à solliciter (excessivement?) certains textes du Code pénal, pensés dans une optique de protection des biens *matériels* contre leur soustraction ou leur détérioration. On songe notamment au "vol" (*soustraction* frauduleuse d'une *chose* appartenant à autrui) applicable, en principe, à des objets matériels et appliqué désormais -sans unanimité- à des biens immatériels tels que des données et programmes informatiques. Ainsi, des juges -dont on attend toujours plus qu'ils soient les gardiens de nos libertés dans un monde en mutations- n'ont pas hésité à interpréter la loi pénale, non plus strictement, mais de façon évolutive, voire analogique. Internet ne fait qu'accentuer ce phénomène, qui pose question au regard du principe de légalité des infractions et des peines (*nullum crimen sine lege, nulla poena sine lege*).

Une autre difficulté tient au fait que le droit pénal est, par essence, un droit national, alors qu'Internet est un phénomène sans frontière. Des règles existent certes pour résoudre d'évidents conflits de lois (quelle loi appliquer?) et de juridictions (quel est le tribunal compétent?). Mais on devine aisément combien leur mise en oeuvre se heurtera souvent à d'insurmontables obstacles pratiques: difficultés d'identification de l'émetteur du message litigieux, possibilité d'oeuvrer à partir d'un paradis électronique (entendez: où la loi pénale est plus laxe...), inutilité d'une sanction frappant un individu résidant à l'autre bout du monde, etc.

En théorie, la loi pénale belge est applicable à toutes les infractions commises sur le territoire du Royaume (art. 3 du Code pénal). C'est le principe, bien connu, de territorialité du droit pénal: dès que quelqu'un, Belge ou étranger, peu importe sa nationalité, commet une infraction sur le territoire de la Belgique, il peut être poursuivi et le juge saisi statuera selon le droit belge. La jurisprudence considère, du reste, que le juge belge est compétent pour statuer sur une infraction dès l'instant où un de ses éléments constitutifs a été commis en Belgique.

En revanche, l'infraction commise hors du territoire du Royaume par des Belges ou par des étrangers n'est punie en Belgique que dans les cas déterminés par la loi (art. 4 du Code pénal). Sauf circonstances exceptionnelles (atteintes à la sûreté de l'Etat...), les infractions commises à l'étranger ne sont poursuivies que si l'inculpé est appréhendé en Belgique. Souvent aussi, la compétence du juge est soumise au principe de la double incrimination.

Ainsi, supposons qu'un message à caractère raciste ou incitant à la violence soit "lancé" sur le réseau à partir de l'Allemagne et reçu en Belgique. On peut penser que, dans ce cas, l'incitation à la haine ou à la violence est réalisée en Belgique de sorte qu'un élément constitutif de l'infraction est bien localisé sur le territoire du Royaume. Le juge belge est donc compétent pour statuer sur l'infraction sur la base de l'article 3, c'est-à-dire sans que les conditions plus strictes de l'article 4 (double incrimination, présence de l'inculpé sur le territoire du Royaume...) doivent être remplies. Cette solution s'inspire de la jurisprudence se-

lon laquelle, en cas d'infractions commises à la radio ou à la télévision, "l'infraction est supposée accomplie en tout lieu où pareille diffusion a pu être reçue ou entendue".

En bref, on a beau dire qu'une infraction reste telle même si elle est perpétrée dans "l'espace virtuel", il est tout de même permis de se demander si les Etats auront toujours les moyens de faire respecter leur loi pénale. Apparaît ainsi la nécessité de renforcer la coopération entre Etats (pour favoriser les extraditions, l'exequatur des décisions de justice étrangères, la collaboration judiciaire et policière...). Mais il ne faut pas se leurrer: la route promet d'être longue tant sont importantes les différences de valeurs et de sensibilités d'un pays à l'autre. De toute évidence, les libertés les plus élémentaires -notamment la très concernée liberté d'expression- ne sont pas conçues de la même façon, loin s'en faut, en Chine, en Algérie, aux Etats-Unis, en Europe, en Corée, au Congo...

Enfin, la question de l'imputation des responsabilités suscite également bien des interrogations. Parmi les multiples intervenants dans la communication électronique, qui doit être tenu pour responsable des informations illicites diffusées ou échangées via Internet? L'un des intermédiaires techniques? Si oui, lequel? Le serveur qui héberge et diffuse l'information, le fournisseur d'accès qui se borne à permettre à ses clients d'accéder au réseau, l'opérateur qui loue ses lignes de télécommunication et assure le transport à distance de l'information? Ou la responsabilité doit-elle peser uniquement sur l'auteur du message litigieux, qui peut se trouver à l'autre bout de la planète et dont il n'est pas toujours aisé d'établir l'identité?

Au fil des cas d'espèce qui leur sont soumis, les juges apportent des éléments de réponse à ces questions, aussitôt commentés par les auteurs. Ainsi, peu à peu, se forme un corpus de principes et de règles, et se réduit la part d'insécurité juridique.

La plupart des questions évoquées se retrouvent en ce qui concerne l'action civile en réparation. Si l'objectif du droit pénal est de rechercher, poursuivre et punir les auteurs d'infractions, le droit de la responsabilité civile vise, lui, à permettre l'indemnisation des victimes. Ici aussi, en cas de litige faisant intervenir des ressortissants de divers Etats, on se référera aux règles en vigueur pour résoudre les questions relatives à la loi applicable et au tribunal compétent. Ici aussi, les problèmes d'identification, de preuve et d'imputation sont épineux. Ici aussi, il appartient au juriste de trouver les solutions adéquates, à la lumière du droit en vigueur et, au besoin, en faisant preuve d'imagination pour forger des solutions originales.

En attendant que des progrès soient accomplis sur le terrain juridique -ou, en priorité, sur le plan politique, car nombre de problèmes à résoudre sont du ressort de la volonté politique-, on retiendra, ici aussi, de possibles solutions d'ordre technique. On songe en particulier aux dispositifs de contrôle et de filtrage des contenus circulant sur le Net.

Parmi les solutions développées, on peut mentionner le système dit "de la liste noire" (blocage de l'accès aux sites spécifiés; l'efficacité du système de la liste noire paraît faible dans la mesure où il concerne un nombre nécessairement limité de sites), le système dit "de la liste blanche" (possibilité d'accès aux seuls sites spécifiés; cette technique peut présenter une utilité pour certains types d'établissements telles des bibliothèques ou des écoles) et le système dit de "l'étiquetage neutre" (étiquetage des sites, qui reçoivent une 'cote morale', l'option étant laissée à l'utilisateur de tenir compte ou non de l'étiquette ou de la cote). Récemment, a été développé un standard performant de filtrage basé sur le principe de "l'étiquetage neutre", appelé PICS (Platform for Internet Content Selection). Il permet une grande souplesse d'utilisation dans la mesure où il est fondé sur une séparation entre la fonction de classement par codification et celle de filtrage proprement dit des sites. Chaque famille peut ainsi adopter le système de codification de son choix, puis spécifier à l'aide de paramètres ce qu'elle accepte ou refuse, en fonction de sa sensibilité et de ses valeurs. Reste à souligner la nécessité d'atteindre une masse critique de sites et de contenus labellisés pour l'efficacité du système PICS.

Conclusion

Qu'il nous soit permis, en guise de conclusion, d'évoquer le célèbre mythe de Protagoras. Le dieu Epiméthée est chargé de distribuer facultés et attributs entre les espèces vivantes. Dans son étourderie, il gaspille tout le trésor au profit des seuls animaux. Négligé dans le partage, l'homme "reste nu, sans chaussures, sans couverture, sans armes". Alors Prométhée, pour sauvegarder l'homme, dérobe aux dieux le feu et l'habileté technique. Mais cela ne suffit pas: dotés de technique, les hommes ne se tirent nullement d'affaire. Encore leur faut-il la morale, l'art politique et le droit. L'ayant compris, Zeus s'empresse de les leur faire porter.

■

(1) Pour un tour d'horizon, voir l'ouvrage collectif, Internet face au droit, cahiers du C.R.I.D. n° 12. Bruxelles, Kluwer, 1997.

(2) On pourrait même songer à voir apparaître à l'écran les données relatives au traitement qui sont consignées dans le registre accessible au public, tenu par l'autorité de contrôle.

(3) A propos de ces diverses solutions techniques, L.F. Cranor. The role of technology in Self regulatory Privacy Regimes, Paper prepared for the NTIA, Déc. 1996.